Posudek vedoucího bakalářské práce

Lukáš Sladký: Key reconstruction from the inner state of RC4

V práci se Lukáš Sladký věnuje rekonstrukci klíče šifry RC4 z jejího vnitřního stavu. Cílem práce bylo prozkoumat dostupnou literaturu, používané postupy vysvětlit a nejlepší z nich naprogramovat.

Šifrování pomocí RC4 se dá rozdělit na dva kroky: inicializaci (KSA) a generování samotného šifrového proudu (PRNA). Při inicializaci se z šifrového klíče vygeneruje prvek S_{256}, který spolu s dvěma ukazateli i, j tvoří vnitřní stav. Následně se generuje posloupnost bytů, která se xoruje s otevřeným textem, čímž vzniká šifrový text. Generování každého bytu deterministicky mění vnitřní stav šifry. Tedy ke zjištění použitého klíče je třeba nejprve invertovat PRNA tolikrát, kolik bytů se doposud vygenerovalo, a pak i KSA.

Práce je rozdělena do šesti kapitol. V první je představena samotná šifra RC4. Ve druhé kapitole je vyřešeno zpětné krokování PRNA do počátečního stavu RC4. Ve zbytku práce se pak řeší inverz KSA. Ve třetí kapitole jsou připomenuty základní definice a věty. Čtvrtá kapitola obsahuje analýzu KSA. Pátá kapitola ukazuje jak využít statistických odchylek v KSA pro získání informací o použitém klíči. Šestá kapitola pak popisuje konkrétní implementaci získání klíče z vnitřního stavu.

Práce vznikla z osmi článků, ale nejedná se o čistě kompilační práci. Některé věty bylo potřeba dokázat podrobněji, než byly dokázány v původním článku, některé ani v literatuře dokázány nebyly. Získané výsledky jsou demonstrovány na příkladech. Součástí práce je i první otevřená implementace popsaného algoritmu.

Cílem práce bylo implementovat nejlepší známý útok. Na to nakonec nedošlo, protože Lukáš přišel na to, že dosud známé postupy se dají zkombinovat tak, že vznikne algoritmus ještě lepší. Drobná potíž, že srovnáváme jen s měřeními dostupnými v literatuře, protože jiné implementace nejsou veřejně dostupné. Jeden příklad za všechny, šestnáctiznakové heslo dokáže výsledná implementace najít s pravděpodobností 7, 7%, kdežto nejlepší známý algoritmus jej dokázal získat jen s pravděpodobností 2%.

S prací studenta v průběhu semestru jsem byl spokojen, aktivně chodil na konzultace a na práci průběžně pracoval. Všechny připomínky, které jsem k textu měl, jsou v něm zapracovány.

Navrhuji proto, aby práce byla přijata jako práce bakalářská a hodnocena stupněm *výborně*.

V Praze dne 1. září 2016 Milan Boháček